

EXHIBIT J
REDACTED
FILED UNDER SEAL

Message

From: Giles Hogben [REDACTED]@google.com]
Sent: 11/29/2018 3:28:17 PM
To: Dave Kleidermacher [REDACTED]@google.com]
CC: Sammit Adhya [REDACTED]@google.com]; Bridget Brennan [REDACTED]@google.com]; Eric Miraglia [REDACTED]@google.com]
Subject: Re: Incognito

I think the combo approach of a quick settings triggered flag plus ephemeral storage mode for writes enforced by a dangerous permission is promising as it would be very close to the Chrome behavior. There are some parallels with the changes we're making to storage in Q. I will write up a 1-pager and talk to jsharkey about this idea.

On Tue, Nov 27, 2018, 9:47 PM Dave Kleidermacher <[REDACTED]@google.com> wrote:

Sounds good, thanks for the thoughts. I agree with both of you that a platform incognito is a tough one - difficult and aggressive. To land it would require some pretty aggressive OOB thinking, resourcing, and solutions. But I agree with Eric's sentiment during the meeting that this would be a massive game changer. If a user could flip the switch at the device (or account) level and have confidence in not having activity tracked in ANY app, it would completely change the way privacy-conscious users and influencers view Google (and Android). One other idea is to tie this to Advanced Protection. We have a plan to augment AP on Android by locking down various important privacy controls like lockscreen and limiting apps to a subset of super-safe apps on Play. So we could offer platform-incognito only for AP users and this would mean that our Play app whitelist would need to ensure all allowed apps are incognito-aware (self-declared and evaluated to obey the requirements/policy therein). Just more food for thought...

On Tue, Nov 27, 2018 at 9:26 PM Sammit Adhya <[REDACTED]@google.com> wrote:
 +Bridget Brennan as FYI

Hi Dave/Giles,

Sorry for the long delay! Climbing out of the email hole after the holiday and some fun user studies on unauth transparency/controls next week.

In a couple weeks I've spent thinking about this, It feels like part of the challenge we face with both Android and Chrome is the definition of incognito and what level of certainty we can provide to users at the platform level vs incognito at the product level. The latter feels, potentially, like an easier problem to solve since we fully control the data lifecycle and can make clear guarantees about the mechanics of how data is used and flows through the product experience.

The platform-level incognito is so much more challenging because it's feels much harder to provide the user guarantees when interacting with 3p (though correct me if I'm wrong!). In addition, we need to figure out what it means for Google products to operate on a platform incognito vs an in-product incognito mode. The exciting part is that we can control the entire stack and at least provide consistency in how things operate as well as clear guarantees for Google product experiences on our platforms.

Based on the research we've seen thus far in our Pinecone studies, it's seems clear that users don't have a good sense of identity management (though it's a small sample size). Even the most basic questions around sign-in/sign-out state are completely misunderstood. Users have no idea whether they are signed in or signed out, what it means for their experience, or what is happening in their current state in terms of data collection. It

would be nice to address both scenarios that both Dave/Giles kind of alluded to: users who have a firm understanding of how to manage their identity across platforms/devices, as well as the, likely more common, group of users who want local privacy (especially in NBU markets) and maybe more protections.

I'd love to start capturing some of these concepts and see how they resonate with users. There are a few questions that I think we need to answer as we go through this process:

- What is the company's appetite/risk for an aggressive approach (like the long-term concept you described Dave)? Are we willing to trade data/revenue for user trust and brand reputation?
- How do we want to define incognito/private browsing? Is it purely for local privacy? Is it privacy from Google? Is it privacy from everyone on the data path? Are the definitions different for incognito at the platform-level vs product-level?
- What is the user mental model of what's happening in an incognito session? Do we try and align ourselves with this mental model, or do we try to better educate our users?

Really appreciate these thoughts! I'll work with Eric and Bridget to figure out how we can move some of these concepts forward as we develop the short-term and long-term product strategy. Look forward to working with you all as things develop!

Thanks much,
Sammit

On Tue, Nov 20, 2018 at 2:54 PM Giles Hogben <[REDACTED]@google.com> wrote:

There is some overlap between a more usable guest user and the incognito flag/quicksetting idea. A guest user meets the incognito requirements of ephemeral state and signed-out operation. The difference is that guest users cannot use any state from other users created prior to entering guest mode (e.g. bookmarks, settings) and from what I heard today, incognito mode doesn't keep some kinds of session data such as search queries.

A disadvantage I see of the quicksetting approach is that it's an honor-system approach. This hasn't worked out well in the past for example with Do Not Track in Chrome and the Limit Ad Tracking flag on iOS and Android though these relate to server-side behaviors that are impossible to verify so it might work out differently for incognito. We could do some Play enforcement but it would be really hard to get all apps to implement. If they don't then we have to hedge the description of the control, making it less trustworthy to users "when you enter this mode, some apps will be in incognito, others won't".

Thinking out of the box, I wonder if we could have a hybrid between the two that enforces ephemerality of state. For example, apps that want to save state beyond an incognito mode session (e.g. Gmail) have to obtain a runtime permission. Without this permission, in incognito mode the app has read-only access to storage minus account manager and a fresh private storage partition is created for the duration of the incognito session.

On Tue, Nov 20, 2018 at 12:19 PM Dave Kleidermacher <[REDACTED]@google.com> wrote:
Hi Sammit,

There are two ways I can see a platform-level concept working, one short term and the other long term.

The long term idea I mentioned in the brainstorm meeting - where we are super aggressive about scrubbing all activity from ever leaving the device on any service, perhaps location too, etc.

The shorter term idea would be to add an ephemeral Android quick setting. When the user turns on or off incognito mode, all apps that are "incognito-aware" (declared in app manifest) get notified. When the user turns on device incognito, that would automatically put YT, Search, Maps, etc. into incognito mode. But instead of having each app fall out of incognito mode individually, they would remain in that mode into either the user turns off the device setting or if the device goes idle for some amount of time (or to be more aggressive, we just leave it on and the user must turn it off, like airplane mode, but I'm guessing the 1P apps might not like that). We could then work with top 3P app providers to ensure they add "incognito awareness" to their apps. Any app that declares itself incognito aware would be prohibited from recording your activity when the mode is enabled. When device incognito is enabled, we would warn-on-launch any apps that are not incognito-aware. Just some thoughts.

I think the separate user account idea, which exists on Android but as Giles mentioned is difficult to use/discover and massively inefficient (mostly unusable in anything less than a flagship device) is also hugely important for the shared device threat model but in my mind mostly orthogonal, i.e. the separate account might still want its activity to be incognito for other reasons.

--

BR,
Dave

Dave Kleidermacher
VP, ASAP

--

Sammit Adhya | Privacy and Data Protection | [REDACTED]@google.com | [REDACTED]

--

BR,
Dave

Dave Kleidermacher
VP, ASAP